Notice of Allowability	Application No.	Applicant(s)	
	10/674,878	CURRIE ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed on 5/19/2010*.

2. ☒ The allowed claim(s) is/are *1,2,9,21,27-30,34,37-40 and 42-48*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20100730* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

- Applicant's amendment filed on 5/19/2010 has been entered. Applicant has amended claims 1 and 21 and added claims 47-48. Currently claims 1, 2, 9, 21, 27-30, 34, 37-40, and 42-48 are pending in this application.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ms. Jamie Rossi (Reg. no. 56875) on July 30, 2010.

Application should be amended as follows:

Claim 1 (Currently amended): An apparatus for providing a security status of an on-line service, comprising:

a web page object that is automatically rendered by a browser when a visitor uses the browser to access one or more web pages of the on-line service via a public network; and

a computer including a verification service ~~of a computer~~ that hosts the web page object separately from the one or more web pages of the on-line service, and further controls contents of the web page object,

wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status through the automatic rendering of the web page object by the visitor's browser, and

wherein the verification service causes the contents of the web page object to be changed in accordance with its prior determination of a level of the security status, such that when the verification service determines, in a first verification operation prior to the visitor's access request, that the on-line service has a first level of the security status, it causes the web page object to have first contents, and when the verification service determines, in a second verification operation prior to the visitor's access request, that the on-line service has a different second level of the security status, it causes the web page object to have different second contents, and thereby automatically controls the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined and changed web page object contents when the visitor requests access to the on-line service, and

wherein the first and second verification operations to determine the on-line service's security status and control the contents of the web page object are performed by the verification service prior to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and

wherein the levels of the security status displayed for the visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the

on-line service are to hackers and other online security threats as determined by the first and second verification operations, and

wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services, and

wherein when the verification service causes the web page object to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser, and

wherein at least one of the first and second verification operations includes scanning the on-line service from a remote address on the network, and

wherein the scanning produces a set of XML files including information about open ports, available service, network protocols, security exposures and vulnerabilities, the information associated with a device providing the on-line service, and

wherein a scan header record associated with the scanning is stored in a database, the scan header record including a date, launch time, duration and a number of vulnerabilities classified by severity level;

wherein the database stores information about generic services expected to be running on the open ports;

wherein the scanning is performed using a scanning engine of the verification service;

wherein the scanning engine parses the set of XML files and stores records of the parsed set of XML files in the database in association with a device record that is further in association with an account number of a provider of the online service;

wherein the apparatus is operable such that the scanning is performed according to a schedule.

Claim 21: (Currently amended) A method for providing a security status of an on-line service, comprising:

hosting a web page object separately from one or more web pages of the on-line service, utilizing a computer;

providing a link to the web page object so that it is automatically rendered by a browser when a visitor uses the browser to access the one or more web pages of the on-line service via a public network;

providing an indication of the security status of the on-line service to the visitor via the automatic rendering of the web page object by the visitor's browser, wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status; and

changing the contents of the web page object to be automatically rendered and displayed in accordance with a determination of a level of the security status, including:

in a first verification operation prior to the visitor's access request, causing the web page object to have first contents if the on-line service has a first level of the security status, and

in a second verification operation prior to the visitor's access request, causing the web page object to have different second contents if the on-line service has a different second level of the security status,

thereby automatically controlling the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined web page object contents when the visitor requests access to the on-line service,

wherein the first and second verification operations to determine the on\-line service's security Status and control the contents of the web page object are performed prior, to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and

wherein the levels of the security status displayed for the visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the on-line service are to hackers and other online security threats as determined by the first and second verification operations, and

wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services, and

wherein, when the web page object is caused to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser, and

wherein at least one of the first and second verification operations includes scanning the on-line service from a remote address on the network, and

wherein the scanning produces a set of XML files including information about open ports, available service, network protocols, security exposures and vulnerabilities, the information associated with a device providing the online service, and

wherein a scan header record associated with the scanning is stored in a database, the scan header record including a date, launch time, duration and a number of the vulnerabilities classified by severity level;

wherein the database stores information about generic services expected to be running on the open ports;

wherein the scanning is performed using a scanning engine of the verification service;

wherein the scanning engine parses the set of XML files and stores records of the parsed set of XML files in the database in association with a device record that is further in association with an account number of a provider of the online service;

wherein the scanning is performed according to a schedule.

Allowable Subject Matter

2. Claims 1, 2, 9, 21, 27-30, 34, 37-40 and 42-48 are allowed.

The following is an examiner's statement of reasons for allowance:

Claims 1 and 21are allowed because the prior art does not teach the combination of limitations as submitted and discussed in the response filed by applicant on 5/19/2010 (see pages 10-13). Dependent claims are allowed due to dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F 9:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 5712723859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435